



Manual de Instalação

Software do TOKEN Aladdin pro 72k

(SafeNet Authentication Client 8.0 SP2)

Para o funcionamento do Token Aladdin pro 72k, deve ser instalado o **Software do Token Aladdin pro 72k** disponível para download no seguinte endereço <http://www.portalautomacao.com.br> após fazer o download do arquivo de instalação siga as orientações abaixo:

Sistemas Operacionais:

Microsoft Windows 2000
Microsoft Windows XP
Microsoft Windows Vista
Microsoft Windows 7

Para confecção desse manual, foi utilizado o Sistema Operacional Windows XP Professional com SP2 (Service Pack 2). Algumas divergências podem ser observadas caso a versão do seu ambiente seja superior ou inferior a esta. **Só conecte o eToken pro 72k na porta USB do computador no final da instalação do programa SafeNet Authentication Client 8.0 SP2.**

eToken Aladdin pro 72k



O SafeNet Authentication Client 8.0 SP2 deve ser instalado em cada computador em que um dispositivo eToken for utilizado. A instalação deve ser realizada por um usuário com privilégios de administrador.

Se encontrar algum problema durante a instalação, registro ou operando este produto, tenha certeza que leu toda a documentação. Se mesmo assim não conseguir resolver o problema, contate seu fornecedor ou o Suporte Aladdin.

1. Feche todos os aplicativos;
2. Clique duas vezes no arquivo **SafeNetAuthenticationClient-x32-x64_8.00-SP2**;
O Assistente de Instalação do SafeNet Authentication Client 8.0 SP2 Setup será aberto.
3. Clique em Next (Avançar).

Se o SafeNet Authentication Client 8.0 SP2 já estiver instalado, a reparação será iniciada; (Figura 1)



Figura 1 - Assistente de instalação

4. Se o SafeNet Authentication Client 8.0 SP2 não estiver sido instalado no seu computador, a caixa de diálogo **Select interface language** (Escolha o idioma da interface) será exibida; (Figura 2)



Figura 2 - Selecione a linguagem

5. Na lista suspensa, escolha o idioma em que SafeNet Authentication Client 8.0 SP2 será instalado, escolha a opção Portuguese (Português), e clique em **Next**.

O Contrato de Licença será exibido. Selecione a opção **I accept the license agreement** (Aceito o contrato de licença), e clique em **Next**; (Figura 3)

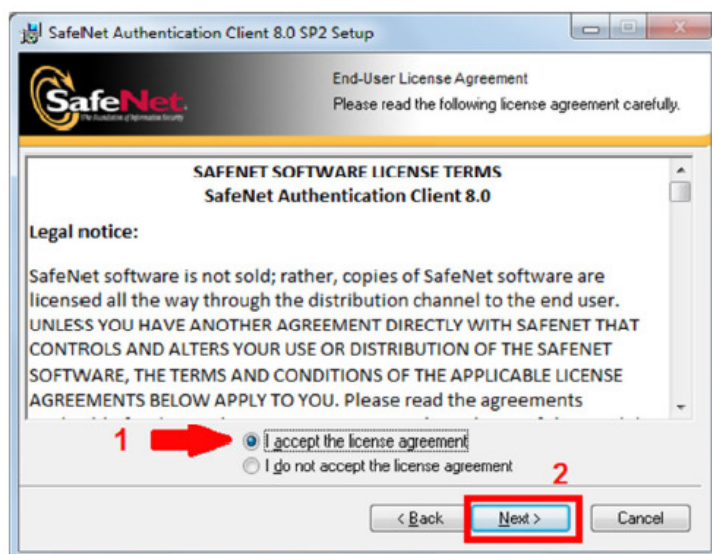


Figura 3 - Contrato de Licença

6. Será aberta uma tela para escolher qual o tipo de instalação desejada, deixe a primeira opção selecionada (**Standard**) e clique em **Next**; (Figura 4)

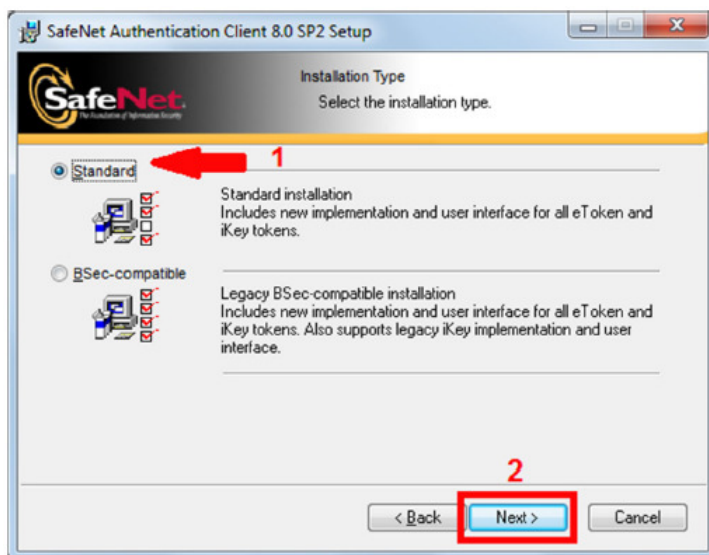


Figura 4 - Escolha de Instalação do driver

7. Será aberta uma janela para escolher a pasta de destino onde o programa será instalado, não há necessidade de alteração, clique em **Next** para iniciar a instalação; (Figura 5)

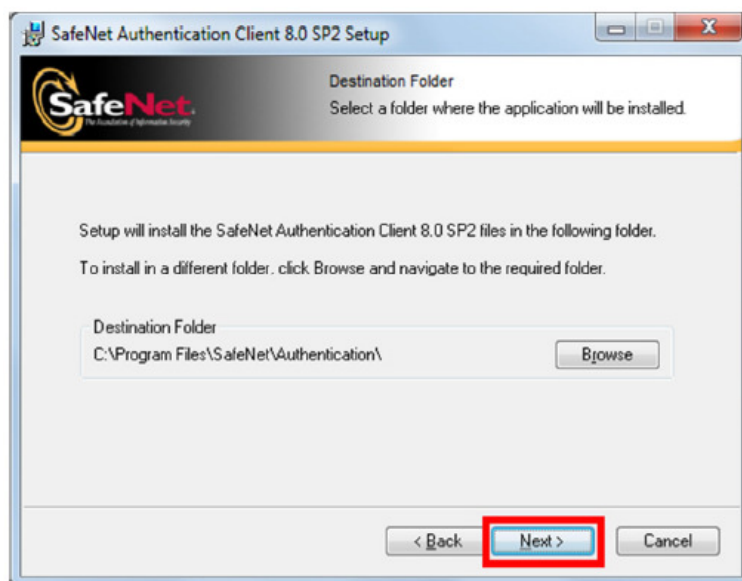


Figura 5 - Caixa de destino do arquivo de instalação

8. Durante a instalação, uma janela Updating System (Atualizando o Sistema) será exibida, apresentando o andamento da instalação; (Figura 6)

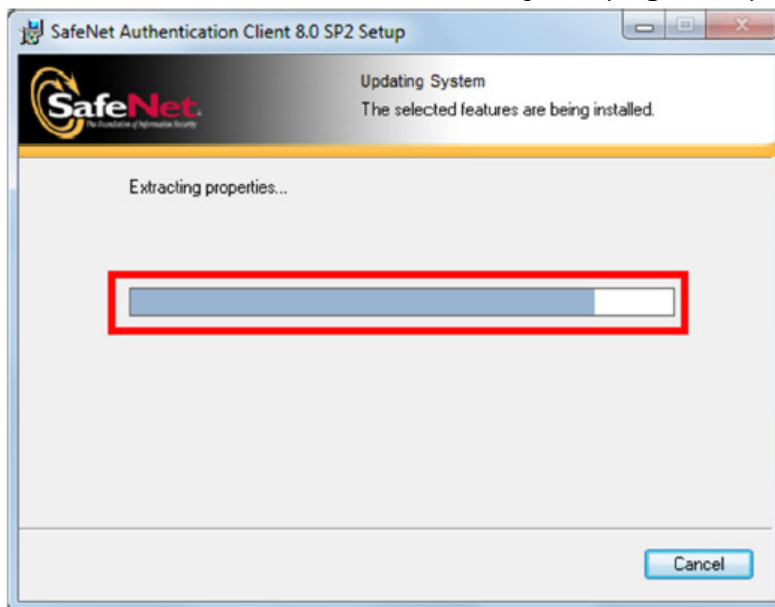


Figura 6 - Updating System

9. Quando a instalação for concluída, a seguinte mensagem será exibida **SafeNet Authentication Client 8.0 has been successfully installed** (SafeNet Authentication Client 8.0 foi instalado com sucesso), clique em **Finish** (Finalizar); (Figura 7)

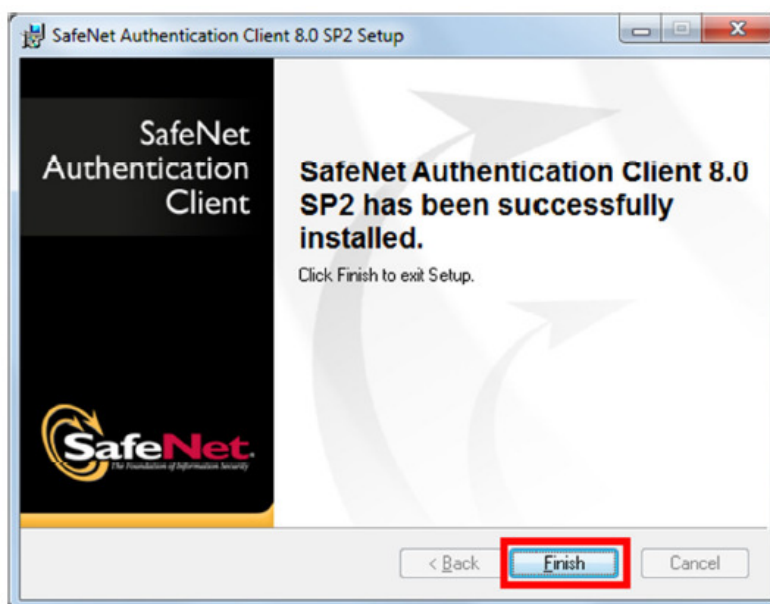


Figura 7 - Finalizando instalação

OBS: Se o TOKEN já possui o certificado não é necessário fazer o procedimento de inicialização.

INICIALIZANDO O TOKEN (PROCEDIMENTO RECOMENDADO)

ESTE PROCEDIMENTO APAGARÁ TODOS OS CERTIFICADOS CONTIDOS NO ETOKEN PRO 72K.

Todos os dispositivos eToken são configurados com a senha original de fábrica 1234567890. Para garantir alta segurança, é fundamental que o usuário altere a senha do eToken para uma senha particular no ato de seu recebimento.

A senha do eToken alterada será a utilizada em todos os seus aplicativos. O usuário é responsável por memorizar a senha do eToken, pois sem ela, não será possível utilizá-lo.

A criação de uma senha de administrador no eToken permite o seu desbloqueio (através da senha PUK), redefinindo uma nova senha para o usuário, e caso a mesma seja esquecida, é com a senha de administrador que será criada novamente a senha de usuário. Por isso é recomendado o procedimento de Inicialização.

Quando aparecer a mensagem “A senha não é mais válida” e/ou solicitando para alterar a senha e pedindo a atual, clique no botão cancelar e siga as orientações das figuras abaixo, no final do procedimento seu eToken estará pronto para receber o certificado digital.

Para criar a senha de **USUÁRIO** e de **ADMINISTRADOR**, o padrão de exatos 08 dígitos, misturando letras, números e caracteres especiais (exemplo: @,#,\$,%,*) é necessário, exemplo de senha: abc1234@.

Depois de instalado o software SafeNet Authentication Client 8.0 SP2, conecte o eToken pro 72k na porta USB do computador e siga as orientações abaixo.

O procedimento de Inicialização apagará todo conteúdo do token, antes de iniciar esse procedimento, certifique-se que o token não possui nenhum certificado digital gravado.

A Inicialização do token é necessária uma única vez, depois de inicializado e com certificado digital gravado, não é necessário fazer o procedimento de inicialização. O eToken pro 72k pode ser utilizado em várias máquinas, havendo a necessidade de instalar o software SafeNet Authentication Client 8.0 na máquina em que se deseja utilizar, para instalar software SafeNet Authentication Client 8.0 siga as orientações a partir da pag 1.

Inicializando eToken

1. Abra o gerenciador do eToken, clique na opção SafeNet Authentication Client Tools; (Figura 8)



Figura 8 - Abra o gerenciador do Token

2. Clique na opção "Vista avançada", (Figura 9);

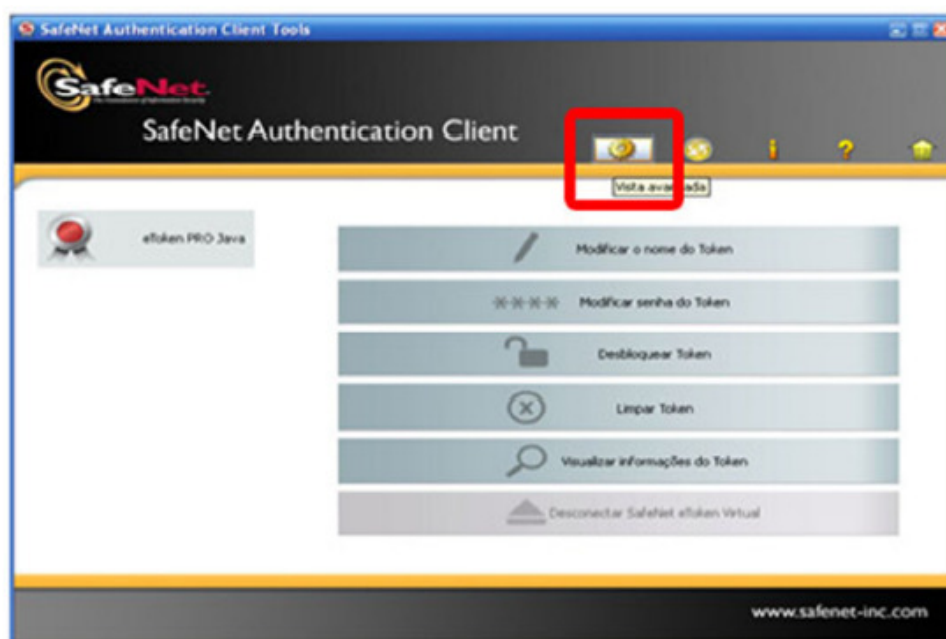


Figura 9 - Vista avançada

3. Selecione a terceira opção "eToken PRO Java", em seguida clique em "Inicializar token", (Figura 10);

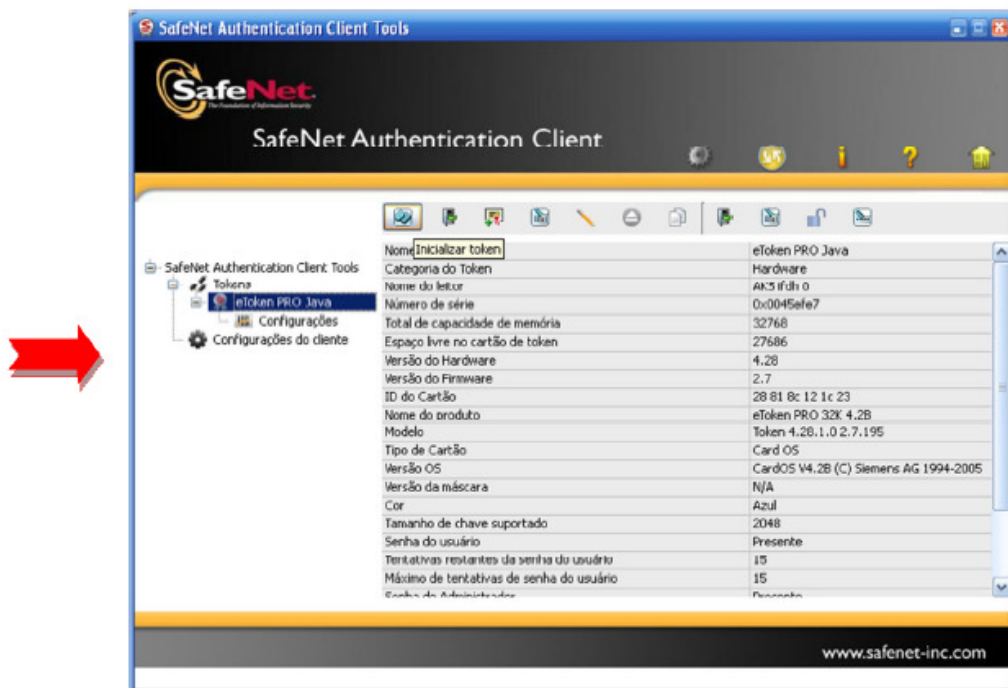
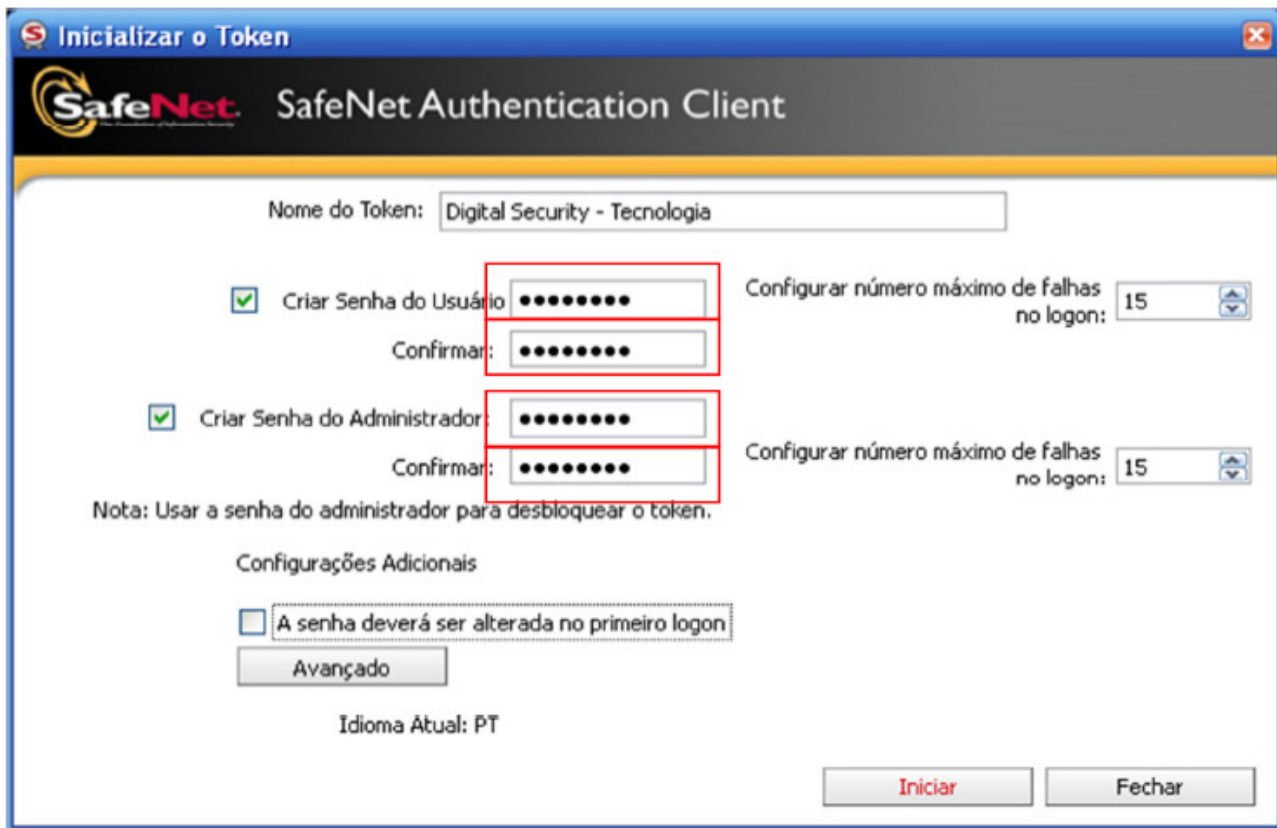


Figura 10 - Inicializar Token

4. Abrirá uma janela, no campo Criar Senha do Usuário apague o que está preenchido e crie uma nova senha de usuário, confirme a nova senha no campo Confirmar, clique na opção Criar Senha do Administrador e crie uma senha diferente da senha de usuário, confirme a senha de administrador no campo Confirmar; Desmarque a opção "A senha deverá ser alterada no primeiro login" e clique no botão Iniciar. Lembrando que para criar as senhas de **USUÁRIO** e **ADMINISTRADOR**, a mesma deve seguir um padrão de exatos 08 dígitos, misturando letras, números e caracteres especiais (@,#,\$,%,*), exemplo de senha: abc1234@. **É de responsabilidade do cliente memorizar e guardar as duas senhas.** (Figura 11)



The image shows the 'Inicializar o Token' (Initialize Token) window of the SafeNet Authentication Client. The window has a blue title bar and a header with the SafeNet logo and 'SafeNet Authentication Client'. The main area contains the following elements:

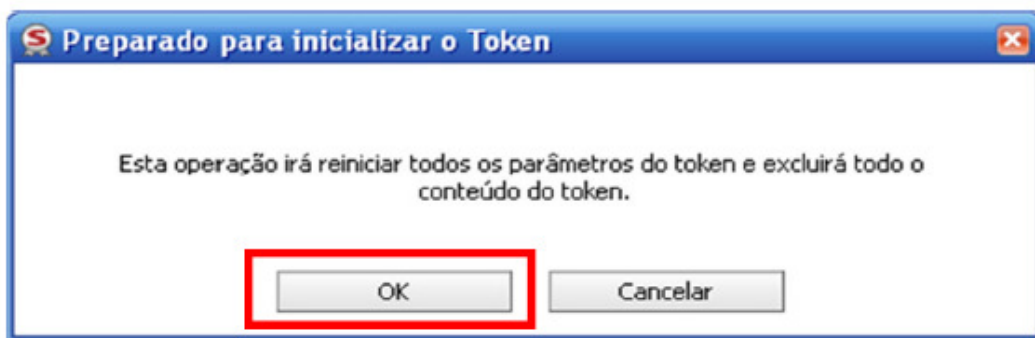
- A text box for 'Nome do Token:' with the value 'Digital Security - Tecnologia'.
- Two checked checkboxes: 'Criar Senha do Usuário' and 'Criar Senha do Administrador'.
- For each checked checkbox, there are two password fields (one for the password and one for confirmation) and a spinner box for 'Configurar número máximo de falhas no logon:' set to 15.
- A note: 'Nota: Usar a senha do administrador para desbloquear o token.'
- A section 'Configurações Adicionais' with an unchecked checkbox 'A senha deverá ser alterada no primeiro logon' and an 'Avançado' button.
- The language is set to 'Idioma Atual: PT'.
- Buttons 'Iniciar' and 'Fechar' at the bottom right.

Red boxes highlight the password and confirmation fields for both user and administrator.

Figura 11 - Criar senhas

As senhas não podem ser iguais e devem conter exatamente 8 (oito) dígitos, misturando letras, números e caracteres especiais.

5. Abrirá uma janela com a seguinte mensagem: "Esta operação irá reiniciar todos os parâmetros do token e excluirá todo o seu conteúdo."; Caso tenha algum certificado gravado dentro do token, o mesmo será perdido.
De "Ok" para continuar. (Figura 12)



The image shows a small dialog box titled 'Preparado para inicializar o Token'. It contains the following elements:

- A message: 'Esta operação irá reiniciar todos os parâmetros do token e excluirá todo o conteúdo do token.'
- Two buttons: 'OK' and 'Cancelar'.

The 'OK' button is highlighted with a red box.

Figura 12 - Preparado para inicializar

6. Se as senhas conferirem e se enquadrarem no padrão de qualidade, aparecerá a seguinte tela; (Figura 13)

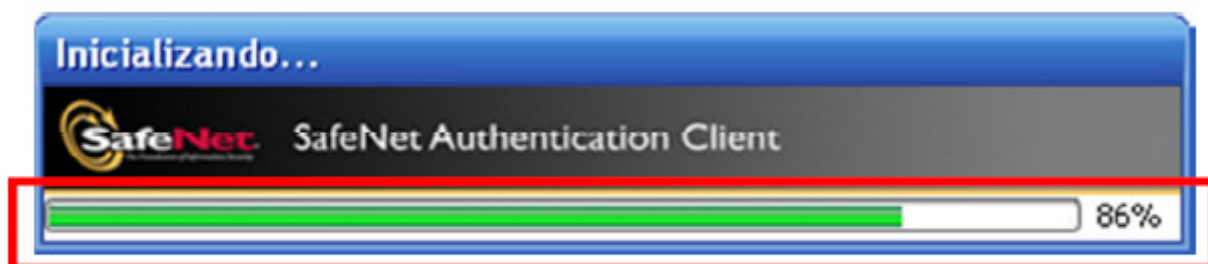


Figura 13 - Inicializando

7. Ao finalizar o procedimento de inicialização aparecerá a seguinte mensagem "O Token foi inicializado com êxito". Clique no botão "Ok" e seu eToken pro 72k está pronto para receber o certificado digital. (Figura 14)

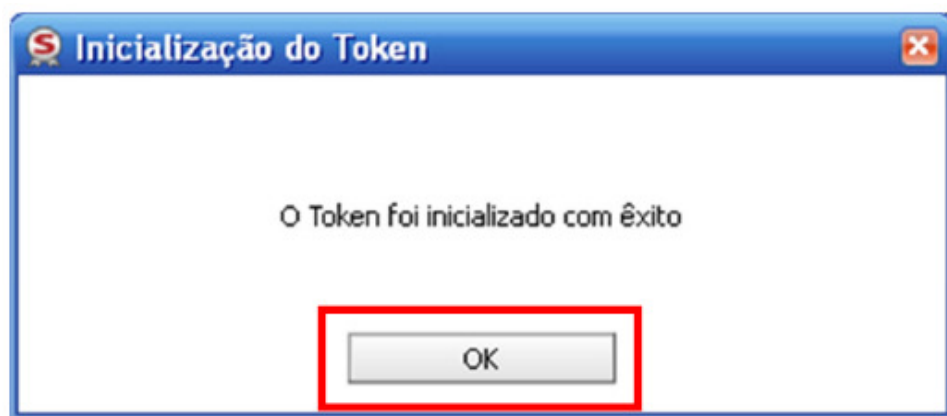


Figura 14 - Token inicializado com êxito

8. Obs: A senha de USUÁRIO é a que será utilizada no dia-a-dia, a senha de ADMINISTRADOR é uma senha de segurança, só será utilizada em caso de perda da senha de USUÁRIO ou bloqueio do eToken, o próprio cliente é responsável por memorizá-las, a PORTAL Automação não se responsabiliza pela perda da senha ou bloqueio do eToken, sendo que a PORTAL Automação não fica com nenhuma senha do cliente.

Como Obter seu Certificado nos Correios

Entrar no seguinte endereço:

http://www.correios.com.br/produtos_servicos/certificacaoDigital/default.cfm

Os Correios comercializam os certificados digitais da Autoridade Certificadora SERPRO/RFB para Pessoa Física e Pessoa Jurídica.

Para adquirir seu certificado digital basta seguir os passos:

1. Escolha no menu ao lado a opção "Solicitar Certificado Digital", no novo menu escolha "Solicitar" de acordo com o segmento:
Pessoa Física: e-CPF tipo A1 ou A3;
Pessoa Jurídica: e-CNPJ tipo A1 ou A3;
Pessoa Jurídica exclusivo para ME (Micro-empresas) e EPP (Empresas de Pequeno Porte): e-CNPJ ME EPP A3

Observação: se optar pelo A3, é necessário que o interessado, antes da solicitação, adquira um dispositivo de armazenamento – token e instale o driver de controle correspondente. Para adquirir o seu dispositivo de armazenamento entre em contato no site www.portalautomacao.com.br.

2. Após efetuar a solicitação, imprima 2 cópias do termo de titularidade que é gerado automaticamente no final da etapa de solicitação. O termo de titularidade só deverá ser assinado na presença do Agente Registrador dos Correios em uma das agências credenciadas.

Observação: memorize a frase senha, pois esta será necessária para baixar o certificado digital.

3. Compareça em uma Agência dos Correios credenciada para prestação do serviço com 2 cópias do termo de titularidade e 1 cópia da documentação.
4. Na agência dos Correios, o solicitante assina o Termo de Titularidade na presença do Agente Registrador dos Correios e submete-se à validação dos seus documentos para a autorização (aprovação) do seu certificado digital. Na agência também ocorre o pagamento da taxa referente ao certificado digital (dinheiro, cheque e cartões) - o comparecimento presencial do titular do certificado é uma exigência da ICP/Brasil.

5. Após a autorização na agência, o certificado digital está imediatamente pronto para ser baixado pelo site dos Correios. A baixa deve ocorrer no mesmo computador onde foi feita a solicitação, com o mesmo usuário conectado (login do sistema operacional) e desde que o computador não tenha qualquer tipo de atualização (seja de software ou hardware) entre a fase de solicitação e a baixa.

Recomendamos que a solicitação, a aprovação na agência e a baixa ocorram no mesmo dia, afim de evitar transtornos para o solicitante.

Araxá (MG), março de 2012.